QR4431 User Manual

Contents

1. Abstract

This datasheet describes reader specification, how to install the Reader, how to use the DEMO software, and how to use API functions.

2. Reader specification

A suit of the reader includes: 1pcs reader, 1pcs antenna (Inside), 1pcs RS232/USB cable. Shown as below:

Figure 1 a suit of the reader

2.1. Reader specification

Electrical spec.:

- Operation frequency: 920-925MHz(CHN); 902-928MHz(FCC)

- Radio regulator: CHN/FCC

- Protocol: EPC C1 GEN2 (ISO18000-6C)

- Reader range: tag dependent

- Write range: 70% reader range

- ANT port: 1

- ANT number:1

- Interface Port: RS232

- Output power: 15-27dBm

- Frequency stability: ±10%ppm

- Power: 5VDC/500mA by power of usb interface

- Power consumption: 2.5Watts

Environment:

- Operating temperature: -10 - 50℃

- Storage temperature: -25 - 65℃

- Operating Humidity: 5 to 95% RH non condensing

Mechanical spec.:

- Dimension: 145*130*30mm

- Weight:350g

3. Driver installation guide

Install CP210x_VCP_Win2K_XP_S2K3 setup file ,Then plug usb cable o reader in usb interface of PC. The PC will find a new hardware and install the driver if connect reader first. Enter the Device Manager and find the virtual COM.

4. Reader demo software

4.1. Installation the demo software

. Before run the demo software, donet framework2.0 or up need to install .then double click QuanrayReaderDemo.exe start the demo.

4.2. Explanation of the demo software

The main window of the demo software, as follow:

The data for the inventory command display in the right corner window.

The left window displays the detail for the reader and client control.

4.3. Select Reader connection

When open the demo software first, a window like the following picture displays, you can select the connection with the reader in this window and you can change the connection parameter in the edit box.
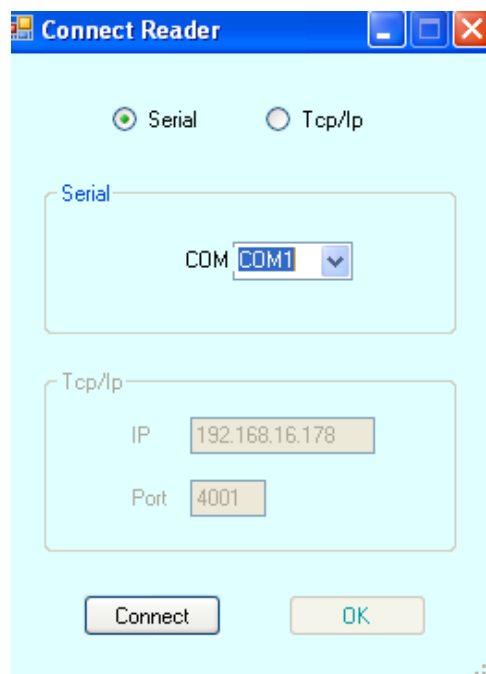
Click the connect button, the main window of the demo software will display if the demo software set up connect success with the reader.

4.4. Query parameters set
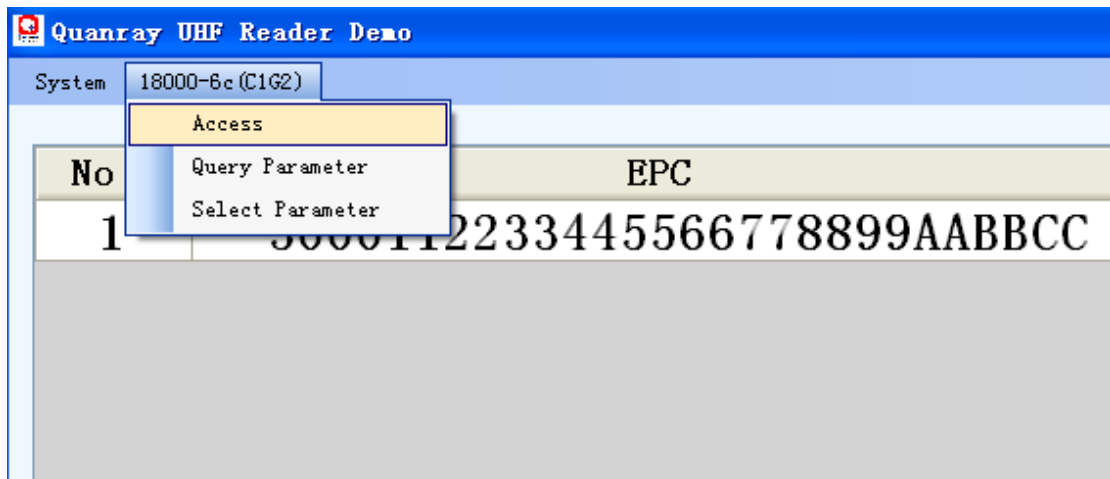
Click Query Manu:
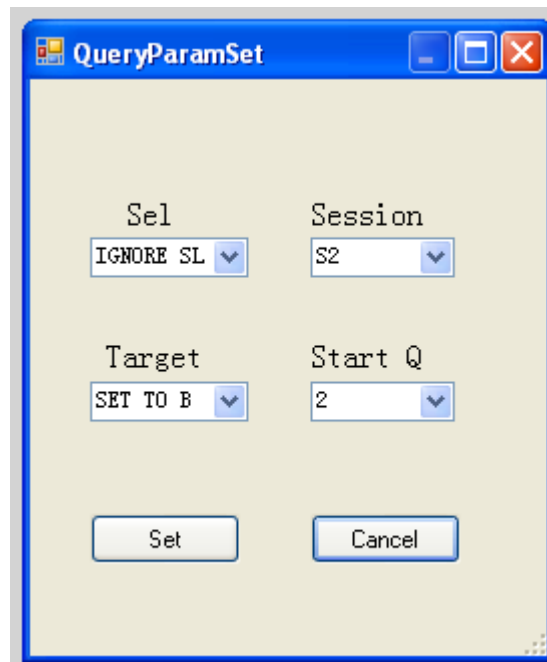
Above display inventory default parameters

4.5. Select parameters set
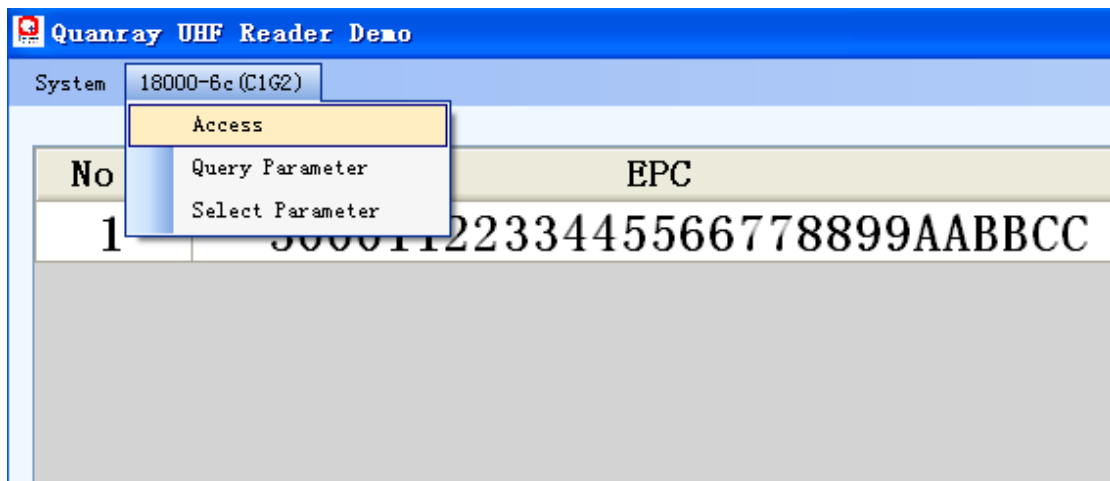
The host may change the select parameter saved in the reader.. If you click the

RstSelect button, the reader will reset the default select parameter.

When the Set button is clicked, a window will be opened as follow:
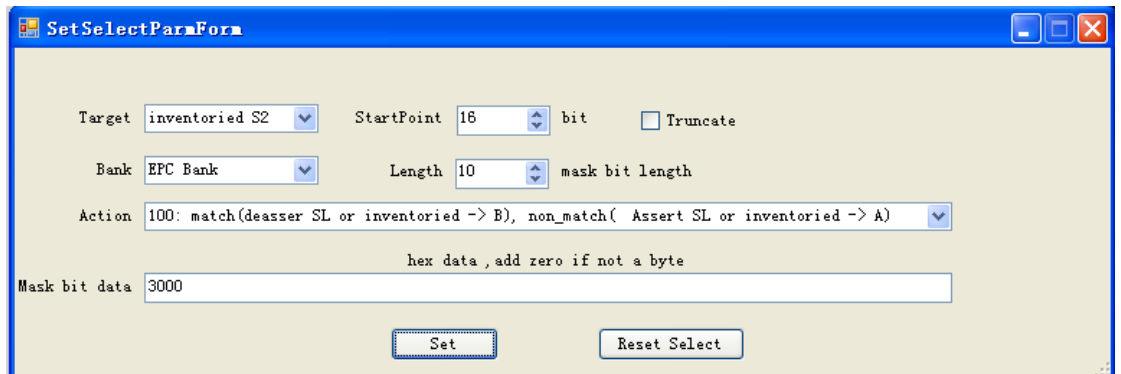
You can change the select parameter according to your need, click the Set button to write select parameter to reader.

4.6. Inventory way select
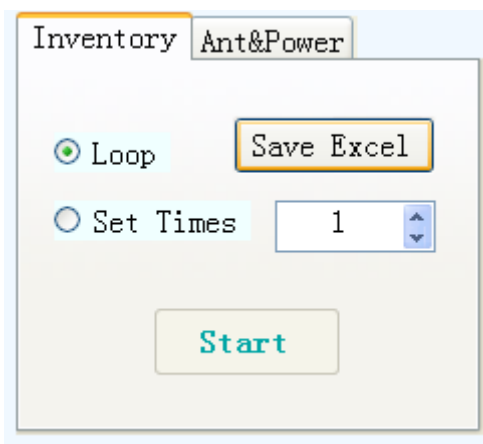
Demo software have two way to get epc bank data by inventory.

Loop: click start button to start inventory operate until click start button again

set times: inventory the tag counts to a set value.

Default: once.
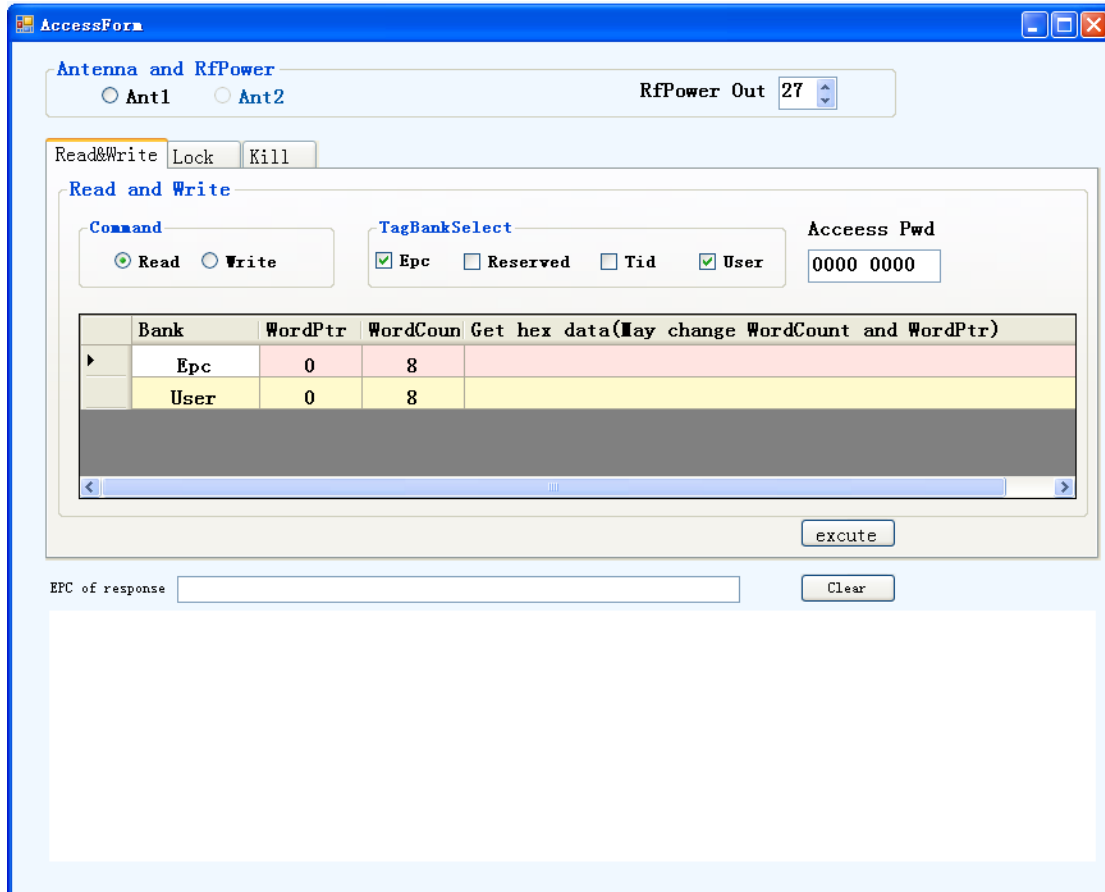
4.7. RF power output set and antenna select
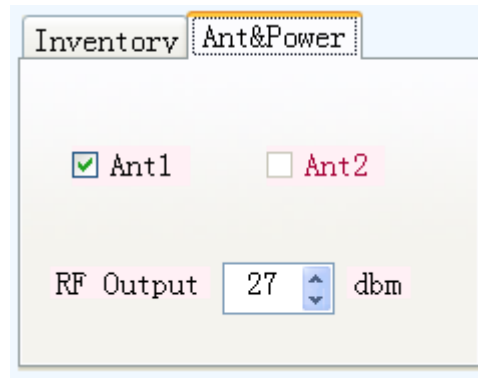
The demo software will get the antenna connection status after reader set up connection with demo software. If reader checks an antenna, the demo will enable antenna select. The output RF power is between 15 and 27。Only one antenna can be selected in this reader..

4.8. Access Function

You can execute read, write, kill, lock subcommand in access command,.

5. Basic protocol packet format

Host to Reader communications follows a Request-Response protocol. The Host sends request packets, and the Reader sends Responses. But the reader can send a information to host initiative.

Request packet format:

Field Name	Description	Length（byte）

0xEE	packet head	1
Packet length	No include packet head and CRC length	2(MSB first)
type	Packet type	1
Payload	Packet data	Whole payload length
CRC check	16-bit CCITT-CRC (MSB first)	2

Response format:

Field Name	Description	Length（Byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length(MSB first)	2
type	Packet type	1
Payload	Packet data	Whole payload length
CRC check	16-bit CCITT-CRC (MSB first)	2

5.1. Command set

5.1.1 Get Reader Info

To get the basic info of the reader, client software should send get reader info request .the reader will response the antenna default status when the reader is running.

Request format:

Field Name	description	Length（byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length	2
0x0a	Get Reader Status COMMAND	1

CRC check	16bit CCITT-CRC (MSB first)	2

Response format:

Field Name	description	Length（byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length	2
0x0a	Get Reader Status COMMAND	1
Reader status	0x00: reader run status check pass。 0xFF:reader reader initial fail	1
Software version	Current Reader software version	2
Hardware version	Current Reader hardware version	2
Antenna status	0b0000 0001　Antenna1 connected 0b0000 0010　Antenna2 connected 0b0000 0100　Antenna3 connected 0b0000 1000　Antenna4 connected	1
Status code	0x01 0x00　CRC check error	2
CRC check	16bit CCITT-CRC (MSB first)	2

Note: reader will send the response when the reader checks some antenna fault.

5.1.2 Set Select

Change the select parameter in the reader. the default select parameter length = 0、Target = 2、Action = 4, that is to say, make all tag was Inventoried and use session S2 and make Inventory flag = B..

Request format:

Field Name	Description	Length（byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length	2

0x06	set select command	1
Target	0x00: Modify Session S0 Inventoried Flag 0x01: Modify Session S1 Inventoried Flag 0x02: Modify Session S2 Inventoried Flag 0x03: Modify Session S3 Inventoried Flag 0x04 Select SL	1
Action	Action / Matching / Non_Matching table (see below)	1
Memory bank	0x00: reserver bank 0x01:epc bank 0x02:Tid bank 0x03: user bank	1
Point	The memory bit address at which to start matching Ms Byte first	2
length	Number of bits to use of Mask Note : 0 implies all tags match	1
mask	Bits to match ,MS bit first	32
Truncate	0x00 :disable truncation	1
CRC check	16bit CCITT-CRC (MSB first)	2

Action sub-table:

Action	Matching	Non_Matching
0x00	Assert SL or inventoried -> A	deassert SL or inventoried ->B
0x01	Assert SL or inventoried -> A	Do nothing
0x02	Do nothing	deassert SL or inventoried ->B
0x03	Negate SL or A-> B,B-> A	Assert SL or inventoried -> A
0x04	deassert SL or inventoried ->B	Assert SL or inventoried -> A
0x05	deassert SL or inventoried ->B	Do nothing
0x06	Do nothing	Assert SL or inventoried -> A
0x07	Do nothing	Negate SL or A-> B,B-> A

Response format:

Field Name	Description	Length（byte）

0xEE	packet head	1
Packet length	No include packet head and CRC length	2
0x06	set select command	1
Command status	0x00：Command execute success 0xFF：Command execute fail	1
Status code	0x01 0x00　CRC check error 0x08 0x00　select list full	2
CRC check	16bit CCITT-CRC (MSB first)	2

5.1.3 Reset Select

Reset Select parameter to default select parameter

Request format:

Field Name	Description	Length（byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length	2
0x07	reset select command	1
CRC check	16bit CCITT-CRC (MSB first)	2

Response format:

Field Name	Description	Length（byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length	2
0x07	reset select command	1
Command status	0x00：Command execute success 0xFF：Command execute fail	1
Status code	0x01 0x00　CRC check error	2
CRC check	16bit CCITT-CRC (MSB first)	2

5.1.4 Inventory Tag

Returns a list of Gen 2 Class1 tags found in the field of the reader. The tags are first selected by the select criteria in the Select List. If the Select List is empty, the default select is used.

Request format:

Field Name	description	Length（byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length	2
0x01	Inventory command	1
RF POWER	15~30	1
Sel	0x00:All tag can be inventoried ;ignore SL(default) 0x01:Only inventory tags with SL NOT set 0x02:Only inventory tags with SL SET	1
session	0x00:Use session S0 for inventory(0x01:Use session S1 for inventory 0x02:Use session S2for inventory（default） 0x03:Use session S3 for inventory	1
Target	0x00:Only inventory Tags with inventoried flag set to A for session 0x01:Only inventory Tags with inventoried flag set to B for session（default）	1
Starting Q	0-15: Sets the number of slots (=2Q) in the first Inventory Round of the Inventory	1
Antenna select	0b0000 0001 Antenna1 0b0000 0010 Antenna2 0b0000 0100 Antenna3 0b0000 1000 Antenna4	1
CRC check	16bit CCITT-CRC (MSB first)	2

Response format:

Field Name	Description		Length（byte）
0xEE	packet head		1
Packet length	No include packet head and CRC length		2
0x01	Inventory command		1
Command status	0x00：Command execute success 0xFF：Command execute fail		1
Tag response num	return tag number		1
Tag response1	Antenna series number	01：antena1 02：antena2 03：antena3 04：antena4	1
	Epc id length	epc id length not include pc　N	2
	Pc		2
	Epc	EPC data	N*2
Tag response2			
……			
Tag response n			
Status code	0x01 0x00　CRC check error 0x02 0x00　Set RX Bitrate error 0x03 0x00　tag no response or timeout 0x04 error_code (error code of tag response) 0x05 0x00　antenna fault 0x06 0x00　Access password error 0x07 0x00　RFpower set error		2
CRC check	16bit CCITT-CRC (MSB first)		2

Note: if Command status execute unsuccessfully, the tag response data ignore.

5.1.5 Read tag

Read allows reader to read part or of a tag's reserved, EPC, TID, or User memory. Read has the following filed:

Memory Bank specifies whether the Read accesses Reserved, EPC, TID, User memory. Read commands shall apply to a single memory bank.

WordPtr specifies the starting word address for the memory read, where words are 16 bits in length. For example WordPtr = 00h specifies the first 16 bit memory word, WordPtr = 01h specifies the second 16 bit memory word.

WordCount specifies the number of 16-bit words to be read..

Access password: when access password of tag is not zero, a valid Access password must be given to enter Secured state to execute read request.

The tag enters secured state to execute command if Tag Access password is not zero.

Request format:

Field Name	Description	Length（byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length	2
0x02	read command	1
RF POWER	15~30	1
Sel	0x00:All tag can be inventoried; ignore SL(default) 0x01:Only inventory tags with SL NOT set 0x02:Only inventory tags with SL SET	1
session	0x00:Use session S0 for inventory 0x01:Use session S1 for inventory	1

	0x02:Use session S2for inventory(default) 0x03:Use session S3 for inventory	
Taget	0x00:Only inventory Tags with inventoried flag set to A for session 0x01:Only inventory Tags with inventoried flag set to B for session(default)	1
Starting Q	0-15: Sets the number of slots (=2Q) in the first Inventory Round of the Inventory	1
Access password	0x00000000 if not application	4
Memory bank And Enable Access password	0x00 : reserver bank 0x01: epc bank 0x02: Tid bank 0x03: user bank	1
WordPtr	Start address point	1
WordCount	Number word to read	1
Antenna select	0b0000 0001 Antenna1 0b0000 0010 Antenna2 0b0000 0100 Antenna3 0b0000 1000 Antenna4	1
CRC check	16bit CCITT-CRC (MSB first)	2

Response format:

Field Name	description		Length（byte）
0xEE	packet head		1
Packet length	No include packet head and CRC length		2
0x02	read command		1
Command status	0x00：Command execute success 0xFF：Command execute fail		1
Tag response num	return tag number		1
Tag response	Tag id length	epc id length not include pc N	1

	Pc		2
	Epc	EPC data	N*2
Read data	Length n	Read data length(16bit) M	1
	Data	Read data content	M*2
Status code	0x01 0x00 CRC check error 0x02 0x00 Set RX Bitrate error 0x03 0x00 tag no response or timeout 0x04 error_code (error code of tag response) 0x05 0x00 antenna fault 0x06 0x00 Access password error 0x07 0x00 RFpower set error		2
CRC check	16bit CCITT-CRC (MSB first)		2

Note: if Command status execute fail, the tag response data ignore.

5.1.6 Write tag

Write allows a reader to write a word in a Tag's Reserved, EPC, TID, or User memory. Write has the following fields:

MemBank specifies whether the Write occurs in Reserved, EPC, TID, or User memory.

WordPtr specifies the word address for the memory write, where words are 16 bits in length. For example, WordPtr = 00h specifies the first 16-bit memory word, WordPtr = 01h specifies the second 16-bit memory word, etc.

Access password: when access password of tag is not zero, a valid Access password must be given to enter Secured state to execute read request.

Enable Access password bit specifies if the tag enters secured state to execute command, when Tag Access password is not zero.

Request format:

Field Name	description	Length（byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length	2
0x03	Write command	1
RF POWER	15~30	1
Sel	0x00:All tag can be inventoried ;ignore SL(default) 0x01:Only inventory tags with SL NOT set 0x02:Only inventory tags with SL SET	1
session	0x00:Use session S0 for inventory 0x01:Use session S1 for inventory 0x02:Use session S2for inventory(default) 0x03:Use session S3 for inventory	1
Taget	0x00:Only inventory Tags with inventoried flag set to A for session 0x01:Only inventory Tags with inventoried flag set to B for session(default)	1
Starting Q	0-15: Sets the number of slots (=2Q) in the first Inventory Round of the Inventory	1
Access password	0x00000000 if not application	4
Memory bank And Enable Access password bit	0x00 : reserver bank 0x01: epc bank 0x02: Tid bank 0x03: user bank	1
WordPtr	Start address point	1
WordCount	Number word to write	1
RFU	0	2
data	Write data	WordCount * 2
Antenna select	0b0000 0001 Antenna1 0b0000 0010 Antenna2 0b0000 0100 Antenna3 0b0000 1000 Antenna4	1
CRC check	16bit CCITT-CRC (MSB first)	2

Response format:

Field Name	description	Length（byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length	2
0x03	Write command	1
Command status	0x00：Command execute success 0xFF：Command execute fail	1
Tag response num	return tag number	2
Tag response	Tag id length epc id length not include pc	1
	Pc	2
	Epc tag id data	N*2
Status code	0x01 0x00 CRC check error 0x02 0x00 Set RX Bitrate error 0x03 0x00 tag no response or timeout 0x04 error_code (error code of tag response) 0x05 0x00 antenna fault 0x06 0x00 Access password error 0x07 0x00 RFpower set error	2
CRC check	16bit CCITT-CRC (MSB first)	2

Note: if Command status execute fail ,the tag response data ignore.

5.1.7 Lock

Read command can allow reader to lock all memory, EPC memory, TID memory, or user memory. Lock command suit for operating one bank.

Lock password, prevent or allow reader / write this password.

Lock individual memory, prevent or allow this individual memory.

Lock permanently this memory.

Only Tags in the **secured** state shall execute a *Lock* command.

Request format:

Response format:

Field Name	description		Length（byte）
0xEE	packet head		1
Packet length	No include packet head and CRC length		2
0x04	lock command		1
Command status	0x00：Command execute success 0xFF：Command execute fail		1
Tag response num	return tag number		2
Tag response	Tag id length	epc id length not include pc	Tag response
	Pc		2
	Epc	tag id data	N*2
Status code	0x01 0x00 CRC check error 0x02 0x00 Set RX Bitrate error 0x03 0x00 tag no response or timeout 0x04 error_code (error code of tag response) 0x05 0x00 antenna fault 0x06 0x00 Access password error 0x07 0x00 RFpower set error		2
CRC check	16bit CCITT-CRC (MSB first)		2

5.1.8 Kill

Kill allow reader prevent tag permanently.
Tag's whose kill password is zero do not execute a kill operation

Request format:

	description	Length（byte）
0xEE	packet head	1
Packet length	No include packet head and CRC length	2
0x09	Kill command	1
RF POWER	15~30	1

Sel	0x00:All tag can be inventoried ;ignore SL(default) 0x01:Only inventory tags with SL NOT set 0x02:Only inventory tags with SL SET	1
session	0x00:Use session S0 for inventory 0x01:Use session S1 for inventory 0x02:Use session S2for inventory(default) 0x03:Use session S3 for inventory	1
Taget	0x00:Only inventory Tags with inventoried flag set to A for session 0x01:Only inventory Tags with inventoried flag set to B for session(default)	1
Starting Q	0-15: Sets the number of slots (=2Q) in the first Inventory Round of the Inventory	1
Enable Access PWD	00：disable 0xff: enable	
Access password	0x00000000 if not application	4
Kill password	0x00000000 if not application	4
Antena select	0b0000 0001　Antena1 0b0000 0010　Antena2 0b0000 0100　Antena3 0b0000 1000　Antena4	1
CRC check	16bit CCITT-CRC (MSB first)	2

Response format:

Field Name	description	Length（byte）	
0xEE	packet head	1	
Packet length	No include packet head and CRC length	2	
0x09	Kill　command	1	
Command status	0x00：Command execute success 0xFF：Command execute fail	1	
Tag response num	return tag number	1	
Tag response	Tag id length	epc id length not include pc	Tag response

	Pc		2
	Epc	tag id data	N*2
Status code	0x01 0x00　CRC check error 0x02 0x00　Set RX Bitrate error 0x03 0x00　tag no response or timeout 0x04 error_code (error code of tag response) 0x05 0x00　antenna fault 0x06 0x00　Access password error 0x07 0x00　RFpower set error		2
CRC check	16bit CCITT-CRC (MSB first)		2

Notice : if Command status execute fail ,the tag response data ignore.

5.1.9 CRC function

```
//

WORD CDemoView::GetCRC16(const CByteArray& InputData, int nLength)

{
    BYTE i;
    BYTE j = 0;
    WORD CRC = 0xffff;
    while(nLength--!=0)
    {
        for(i=0x80; i!=0; i/=2)
        {
            if((CRC&0x8000)!=0)    {CRC*=2;CRC^=0x1021;}
            else CRC*=2;
            if(((BYTE)InputData[j]&i)!=0) CRC^=0x1021;
        }
        j++;
    }
    return ~CRC;
}
```